УДК 004.056

МЕТОДИКА ПОРІВНЯННЯ ЕФЕКТИВНОСТІ СУЧАСНИХ SIEM-СИСТЕМ

О. В. Столова[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

Стаття присвячена розробці нової методики оцінки якості SIEM-систем, що базується на комплексному аналізі характеристик, для вибору найбільш ефективної SIEM-системи.

Ключові слова: SIEM – система, кореляція, методи прийняття рішень

Вступ

В наш час досить актуальною є проблема виявлення інцидентів порушення безпеки інформації на основі аналізу журналів реєстрації подій в інформаційних системах. Кількість журналів реєстрації в сучасних системах обчислюється сотнями, а кількість подій – сотнями тисяч на добу, що обумовлює необхідність застосування спеціальних автоматизованих систем для вирішення цієї задачі – так званих SIEM-систем. Враховуючи те, що на сьогодні на ринку систем захисту присутні десятки різноманітних SIEM-систем, актуальною є задача оптимального (за певними ознаками) вибору SIEM-системи і створення методики оцінки якості, що буде враховувати усі характеристики закладені у систему.

В статті розглянуто вирішення задачі побудови такої методики та її застосування до лідерів ринку SIEM-систем: системи QRadar від IBM та ArcSight від HP.

1. Способи передобробки лог-файлів

Розглянемо, один з основних етапів роботи SIEM-системи – передобробка лог-файлів. У статті [1] акцентовано увагу на тому, що у рішенні QRadar, при відправленні журнала подій в систему, розпізнавання джерела та нормалізація проводиться автоматично, а у ArcSight підключення нових джерел відбувається вручну. IBM QRadar SIEM реалізує аналіз лог-файлів «на льоту», на відміну від рішення HP ArcSight SIEM, що зберігає їх у сховище, а потім обробляє. Розглянувши ці два підходи з точки зору надійності, можемо сказати, що в першому випадку маємо більшу ймовірність помилки 2го роду, тобто вищу ймовірність пропустити подію, що загрожує безпеці організації.

Ще однією відмінністю є те, що QRadar має більше встановлених конекторів, але при цьому більш легка розробка та додавання конекторів до системи у рішенні ArcSight. Слід звернути увагу і на те, що в QRadar обробка подій здійснюється до 7 рівня моделі взаємозв'язку відкритих систем, а в ArcSight – тільки до 4 рівня.

Отже, вже на прикладі розгляду способів передобробки лог-файлів SIEM-системами бачимо, що неможливим є порівняння систем тільки за однією ознакою. Звідси маємо задачу багатокритеріальної оптимізації, а рішенням є не одне рішення, а паретомножина рішень.

2. Методи кореляції подій

Не менш важливим етапом роботи SIEM-системи вважається процес кореляції подій важливих з точки зору безпеки. Розглянемо цей процес докладніше, на прикладі двох SIEM-систем.

Після отримання інформації від джерел, система починає аналізувати цю інформацію. Рішення QRadar є комплексом «з коробки», тому в ньому вже є вбудований набір правил кореляції. Рішення HP ArcSight теж має стандартний набір правил кореляції, але в меншій кількості, оскільки орієнтований на ручне налаштування системи під потреби організації. Дані правила в обох випадках складаються з визначених наборів умов і сценаріїв дій. Правила кореляції розбиті на категорії. Кожне правило окремо можна включити або відключити. Стандартні правила кореляції можна використовувати в якості шаблонів для створення власних.

IBM Qradar надає контекстно-пов'язану і пріоритезовану інформацію про інцидент. Всі спрацьовування різних правил кореляції логічно пов'язаних між собою відносяться до одного інциденту і автоматично об'єднуються в одну подію порушення безпеки інформації, так званий «Offense». Якщо правила кореляції продовжують спрацьовувати, нова інформація додається в цей Offense, а не генеруються нові. У HP ArcSight спочатку це різні зкорельовані події. Пов'язування між собою відбувається вручну. Крім того, зкорельована подія не містить нічого, крім самої події, на відміну від Qradar , де можна побачити одразу

інформацію про активи, інформацію про уразливість, порушника, топологію мережі.

У роботі [2] розглянуто методи, що використовують для створення правил кореляції – це методи на основі знань (зокрема, кінцеві автомати), методи обчислювального інтелекту (зокрема, нейронні мережі), та поведінкові (зокрема, статистичний аналіз).

В рішеннях QRadar та ArcSight враховуть усі переваги та недоліки методів та використовують не один, а декілька методів кореляції.

3. Методи прийняття рішень

Зібравши та обробивши події, що надійшли від обраних джерел, SIEM-система за допомогою методів прийняття рішень, відносить ту чи іншу подію до класу інцидентів інформаційної безпеки. Оскільки в QRadar обробка подій здійснюється до 7 рівня, то система надає більш точний та компактний набір зкорельованих подій, аніж ArcSight.

QRadar та ArcSight використовують декілька методів прийняття рішень. В роботі [3] розглянуто методи, що використовують для прийняття рішень, одними з яких є поведінкові методи , що в процесі своєї роботи порівнюють параметри спостережуваної поведінки з інформацією про нормальну поведінку системи, і випадок значних відхилень розглядається як свідчення наявності атаки. Недоліком даного методу є хибні спрацьовування, які пояснюються в першу чергу складністю точного і повного опису безлічі легітимних дій користувачів. Окрім цього, в SIEM-системах для прийняття рішень використовують методи на основі знань. У статті [4] описано дані методи, як такі, що в контексті заданих фактів, правил виводу і зіставлень, що відображають ознаки заданих атак, виробляють дії по виявленню атак на основі закладеного механізму пошуку. Ці методи працюють з базою знань, в якій включено опис вже відомих атак.

Зважаючи на те, що кожен з цих методів не ідеальний, виробники QRadar та ArcSight використовують поєднання цих методів, задля компенсування їх недоліків.

4. Порівняння SIEM-систем

Табл. 1. Порівняльна таблиця SIEM-систем

Критерії	IBM QRadar	HP ArcSight
Передобробка лог-файлів	Виконується «на льоту»	Зберігає у сховище, а потім обробляє
Додавання конекторів	Розробка та додавання нових конекторів викликає складнощі	Гнучка система розробки та додавання конекторів
Кількість стандартних правил кореляції	Декілька сотень, розробка правил викликає труднощі	Декілька десятків, але має гнучкий механізм розробки правил
Автовизначення джерел подій	Розпізнавання джерела відбувається автоматично	Налаштування проводиться вручну
Можливість моніторингу мережевого трафіку	Повний аналіз мережевого трафіку до 7 рівня	Аналіз мережевого трафіку до 4 рівня
Візуалізація зкорельованих подій	надає інформацію про уразливість, порушника, топологію мережі	Констатує лише факт наявності події
Методи створення правил кореляції	на основі знань, обчислювального інтелекту, поведінкові	
Методи прийняття рішень	Поведінкові, на основі знань	

Висновки

У даній роботі було проведено комплексний аналіз характеристик систем управління подіями інформаційної безпеки (SIEM), на прикладі рішень IBM QRadar та HP ArcSight, що полегшує підбір SIEM-системи під вимоги організації.

В результаті аналізу було виявлено, що неможливим є порівняння систем тільки за однією ознакою, потрібна багатокритеріальна оптимізація, і рішенням є не одне рішення, а парето-множина рішень.

Рекомендовано для великих організацій, холдингових структур, в якості платформи для побудови центру захисту інформації (англ. - secure operation centre (SOC)) використовувати рішення від компанії HP, зважаючи на його гнучкість, багатий функціонал та стійкість до великих навантажень. Організаціям меншого масштабу рекомендовано розглянути рішення від компанії IBM. Це рішення підходить тим організаціям, що використовують стандартні технології обробки інформації, і яким не потрібна специфічна гнучкість платформи для реалізації функцій SOC.

Перелік використаних джерел

1. Тимур Ниязов Сравнение SIEM-решений для построения SOC. Режим доступа: http://www.jetinfo.ru/stati/sravnenie-siem-reshenij-dlya-postroeniya-soc
2. Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1. // Труды СПИИРАН. — 2016. — Вып. 47. С. 5-27 с.
3. Debar H., Dacier M., Wespi A. Towards a taxonomy of intrusion-detection systems //Computer Networks. — 1999. — vol. 31. Issue 8. P. 805-822 с.
4. Браницкий А. А., Котенко И. В.Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. — 2016. — Вып. 45. С. 207-244 с.